

**AMENDMENTS TO THE CLAIMS:**

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method of producing a digital certificate in which a certification authority performs the steps of:
  - grouping together, in a data set, a public key and digital data comprising data identifying the proprietor of said public key and of an associated private key[[],];
  - signing the data set in order to produce a digital certificate[[],]; and
  - storing the signed data set in a computer-readable storage medium,wherein the digital data also comprise data identifying at least one of:
  - means of generating the private key, means of storing the private key on a medium, and means of signing with the private key.
2. (Currently amended) A method according to claim 1, in which the data identifying the means of generating the private key comprise data identifying:
  - a method of generating the private key, and/or
  - hardware on which the method of generating the private key is implemented, and/or
  - a place on which the method of generating the private key is implemented.
3. (Previously presented) A method according to claim 1, in which the data identifying the means of storing the private key comprise data identifying:
  - a method of storing the private key on a medium, and/or
  - hardware on which the method of storing the private key is implemented, and/or
  - a place on which the method of storing the private key is implemented, and/or
  - a storage medium on which the private key is stored.

4. (Previously presented) A method according to claim 1, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

5. (Previously presented) A method according to claim 2, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or
- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

6. (Currently amended) A method according to claim 2, in which the data identifying a method comprise:

- a reference identifying said method of generating the private key, and/or
- an identification of an inventor of said method of generating the private key, and/or
- an indication of a security level of said method of generating the private key according to ISO 15408.

7. (Currently amended) A method according to[[,]] claim 2<sub>1</sub> in which the data identifying a place comprise:

- an identification of said place, and/or
- an identification of a security level of said place according to ISO 15408.

8. (Currently amended) A digital certificate stored in a computer-readable medium, comprising:

- a public key[[,]];
- data identifying a proprietor of the public key and of an associated private key[[,]]; and
- data identifying at least one of means of generating the private key, means of storing the private key on a medium, and means of signature with said private key.

9. (Original) A certificate according to claim 8, of the X509 type according to a standard Information Technology – Open Systems Interconnection – The Directory : Public Key and Attribute Certificate Frameworks, dated March 2000, of the International Telecommunication Union, in which a set of predefined free fields are used to store the digital data identifying:

- a method of generating the private key, and/or
- hardware on which the method of generating the private key is implemented, and/or
- a place on which the method of generating the private key is implemented, and/or
- a method of storing the private key on a medium, and/or
- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored, and/or
- a signature method using the private key, and/or
- a storage medium on which the said signature method is stored.

10. (Previously presented) A method of using a digital certificate according to claim 8, comprising the following steps:

- receiving a message signed with a private key,
- reading, in the digital certificate, data identifying means of generating the private key and/or means of storing the private key on a medium and/or means of signing with the private key,
- deducing therefrom a probability of said private key having been used by a legitimate proprietor of said private key,
- according to said probability, accepting or refusing the electronic message.

11. (Original) A method according to claim 10, in which the message is accepted solely if the probability of the said key having been used by its legitimate proprietor is greater than a predefined value.

12. (Original) A method according to claim 10, in which:

- the message is accepted if the probability is greater than a first value (VB1),
- a confirmation of the said message is requested if the probability is between the first value (VB1) and a second value (VB2) less than the first value, and
- the message is refused if the probability is less than the second value (VB2).

13. (Previously presented) A method according to claim 2, in which the data identifying the means of storing the private key comprise data identifying:

- a method of storing the private key on a medium, and/or
- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored.

14. (Previously presented) A method according to claim 2, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

15. (Previously presented) A method according to claim 3, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

16. (Previously presented) A method according to claim 3, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or
- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

17. (Currently amended) A method according to claim ~~[[4]]~~ 13, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or
- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

18. (Currently amended) A method according to claim 3, in which the data identifying a method comprise:

- a reference identifying said method of storing the private key, and/or
- an identification of an inventor of said method of storing the private key, and/or
- an indication of a security level of said method of storing the private key according to ISO 15408.

19. (Currently amended) A method according to claim 4, in which the data identifying a method comprise:

- a reference identifying said method using the private key, and/or
- an identification of an inventor of said method using the private key, and/or
- an indication of a security level of said method using the private key according to ISO 15408.

20. (Previously presented) A method according to claim 5, in which the data identifying a method comprise:

- a reference identifying said method, and/or
- an identification of an inventor of said method, and/or
- an indication of a security level of said method according to ISO 15408.